ViPNet Programmkontrolle 4.3

Benutzerhandbuch

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Version: 00116-04 34 04 DEU

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt

Einführung

Über dieses Dokument

Das vorliegende Benutzerhandbuch beschreibt das Anwendungsgebiet und die Funktionsweise des Programms ViPNet Programmkontrolle, die Prinzipien und Besonderheiten seiner Arbeitsweise, und beinhaltet Informationen über die Einstellung und Nutzung aller Möglichkeiten des Programms.

Zielgruppe

Das Handbuch ist für Benutzer des Programmpakets ViPNet, das die Anwendung ViPNet Programmkontrolle beinhaltet, bestimmt.

Es wird angenommen, dass der Leser des vorliegenden Handbuchs über Basiswissen im Bereich der Netzwerktechnologien verfügt.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.

Notation	Beschreibung
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Über das Programm

Das Programm ViPNet Programmkontrolle erlaubt es, Netzwerkaktivitäten von Anwendungen zu überwachen, die auf dem Rechner installiert sind. Anwendungen, die im Netzwerk Aktivitäten verursachen (wie zum Beispiel das „Lauschen“ am Port oder das Versenden von Netzwerkpaketen), werden in „Programmkontrolle“ registriert, und ihr Zugriff auf das Netz wird in Abhängigkeit von der Entscheidung des Benutzers entweder erlaubt oder blockiert. „Programmkontrolle“ bietet Schutz vor Gefahren wie zum Beispiel einem unerlaubten Zugriff auf Benutzerdaten oder dem Ausführen von Spyware.

Die Anwendung „Programmkontrolle“ ist eine Komponente der Software ViPNet Client, ViPNet Coordinator, ViPNet Personal Firewall und ViPNet Office Firewall. Dabei ist „Programmkontrolle“ in ViPNet Personal Firewall und ViPNet Office Firewall immer Bestandteil der Software und in ViPNet Client und ViPNet Coordinator nur dann dabei, wenn dies in der Registrierungsdatei festgelegt ist.

Hinweis. Bei Verwendung der Software ViPNet VPN steht das Programm Programmkontrolle ausschließlich als eine Komponente von ViPNet Coordinator zur Verfügung.

Abbildung 1. ViPNet Software, die „Programmkontrolle“ enthält

Systemanforderungen

Eine separate Installation von ViPNet Programmkontrolle ist nicht möglich, deswegen richten sich die Mindestanforderungen an das System für einen erfolgreichen Einsatz der Anwendung an die Anforderungen der Software, die „Programmkontrolle" als Komponente beinhaltet.

Tabelle 3. Mindestsystemanforderungen für die Installation von ViPNet Software

System-anforderungen	ViPNet Software: Coordinator, Office Firewall	ViPNet Software: Client, Personal Firewall
Betriebssystem	Microsoft Windows XP (32-Bit), Server 2003 (32-Bit), Vista (32/64-Bit), Server 2008 (32/64-Bit), Server 2008 R2 (64-Bit), Small Business Server 2008 SP2 (64-Bit), Windows 7 (32/64-Bit), Windows 8 (32/64-Bit), Windows 8.1 (32/64-Bit), Server 2012 (64-Bit), Server 2012 R2 (64-Bit). **Hinweis**. Im Betriebssystem sollte das neueste Updatepaket installiert sein.	
Anwendungen	Wenn Internet Explorer im Einsatz – Version ab 6.0; Abwesenheit anderer Firewalls.	
Prozessor	Prozessor: ein Intel Core 2 Duo oder ein anderer x86-kompatible Prozessoren mit mindestens zwei Kernen wird empfohlen.	
RAM	Mindestens 1024 MB.	Mindestens 512 MB.
Festplatten-Speicherplatz	Mindestens 300 MB bei der Arbeit mit ViPNet Registration Point. Mindestens 1000 MB bei der Arbeit mit ViPNet Coordinator.	Mindestens 150 MB.
Netzwerkadapter	IPv4 unterstützende Adapter	IPv4 unterstützende Adapter

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

1

Allgemeines

Funktionsweise des Programms

Das Programm „Programmkontrolle“ ermöglicht die Überwachung von Netzaktivitäten der auf dem Rechner installierten Anwendungen. Folgende Netzaktivitäten werden erfasst:

- Versuche, eine ausgehende Verbindung herzustellen.
- Versuche, Ports für eingehende Verbindungen zu öffnen.
- Versenden von Datenpaketen ohne vorhergehenden Aufbau einer Verbindung.

Beim Aufspüren einer Netzwerkaktivität wird ein Meldungsfenster eingeblendet, mit dessen Hilfe der Zugriff der Anwendung auf das Netzwerk erlaubt oder abgelehnt werden kann. Das Programm ermöglicht es, Sicherheitsrichtlinien einzurichten, denen zufolge Anwendungen das Ausführen bestimmter Aktivitäten im Netz automatisch erlaubt oder verboten wird, ebenfalls ermöglicht es die Arbeit im nicht-interaktiven Modus (s. Nicht-interaktiver Modus auf S. 56) einzustellen.

Abbildung 2. Die Funktionsweise von „Programmkontrolle“

Nachdem der Benutzer festgelegt hat, ob für eine Anwendung die Arbeit im Netzwerk erlaubt oder verboten ist, wird die betroffene Anwendung von „Programmkontrolle“ registriert. Das bedeutet, dass die gewählte Handlungsweise von „Programmkontrolle“ gespeichert ist und bei jeder weiteren Netzaktivität der betroffenen Anwendung angewandt wird.

Benutzerrechte in ViPNet Programmkontrolle

Bei Netzwerken auf Basis der Software ViPNet Administrator hängt die Möglichkeit zur Änderung der Einstellungen für „Programmkontrolle" vom Umfang der Benutzerrechte des Netzwerkknoten-Benutzers ab (s. Benutzerrechte auf S. 56). Der Umfang der Benutzerrechte wird vom Administrator des ViPNet Netzwerks im Programm ViPNet Administrator festgelegt. Weitere Details über Benutzerrechte beim Einsatz der ViPNet Software finden Sie im Dokument „Klassifikation der Benutzerrechte. Anhang zur Dokumentation von ViPNet".

Bei Verwendung der Software ViPNet VPN, ViPNet Personal Firewall oder ViPNet Office Firewall sind alle Möglichkeiten von „Programmkontrolle" verfügbar.

Hinweis. Wenn die Notwendigkeit besteht, Änderungen an nicht verfügbaren Einstellungen vorzunehmen, wenden Sie sich an den ViPNet Netzwerk Administrator (auf S. 57). Detaillierte Informationen über die Möglichkeit der Anmeldung mit dem Administratorkonto finden Sie im Abschnitt Anmeldung als Administrator in „Programmkontrolle" (auf S. 40).

Bei Netzwerken auf Basis der Software ViPNet Administrator, speziell auf einem Netzwerkknoten mit installiertem ViPNet Client oder Coordinator, gilt:

- Wenn für diesen Netzwerkknoten (s. ViPNet Netzwerkknoten auf S. 57) der maximale Umfang an Benutzerrechten festgelegt ist, dann stehen alle Möglichkeiten des Programms „Programmkontrolle" zur Verfügung.
- Wenn für diesen Netzwerkknoten der Mindestumfang oder ein begrenzter Umfang an Benutzerrechten festgelegt ist, dann gelten folgende Einschränkungen:
  - Es dürfen keine Parameter im Bereich **Einstellungen** geändert werden.
  - Es dürfen keine Parameter im Bereich **Logdatei** > **Logdatei-Einstellungen** geändert werden (mit Ausnahme von Parametern der Gruppe **Logdatei anzeigen**).
  - Es dürfen keine Änderungen am Inhalt der Liste von erlaubten und blockierten Anwendungen vorgenommen werden.
  - Das Programm ViPNet Programmkontrolle darf nicht deaktiviert werden (im Menü **Optionen** sind die Einträge **Programmkontrolle deaktivieren** und **Beenden** nicht verfügbar).

Weitere Informationen über Einschränkungen bei unterschiedlichem Umfang an Benutzerrechten finden Sie im Handbuch „Klassifikation der Benutzerrechte. Anhang zur Dokumentation von ViPNet".

Hinweis. Wenn auf dem Netzwerkknoten eine Aktualisierung der Schlüssel vorgenommen wurde, die Benutzerrechte einschränkt, dann treten diese Einschränkungen in „Programmkontrolle" erst nach einem Neustart des Programms in Kraft.

Benutzeroberfläche von ViPNet Programmkontrolle

Die Benutzeroberfläche des Programms ViPNet Programmkontrolle ist in der folgenden Abbildung dargestellt:

Abbildung 3. Das Hauptfenster von ViPNet Programmkontrolle

Die Zahlen in der Abbildung kennzeichnen folgende Elemente:

1 Die Hauptmenüleiste des Programms.

2 Navigationsbereich, auf dem die Liste von allgemeinen Möglichkeiten des Programms angezeigt ist.

3 Vorschaubereich, auf dem der Inhalt der im Navigationsbereich ausgewählten Bereiche angezeigt ist.

4 Bereich **Programmkontrolle** mit der Übersicht der wichtigsten Funktionsbereiche des Moduls.

5 Bereich **Registrierte Anwendungen**. Ermöglicht die Anzeige von Informationen über Anwendungen, die von „Programmkontrolle“ registriert sind.

Im Bereich **Registrierte Anwendungen** können der Zugriffsmodus einer registrierten Anwendung auf das Netzwerk geändert (s. Netzzugang von Anwendungen einstellen auf S. 35) oder eine Anwendungsregistrierung zurückgenommen werden (s. Eine Anwendung aus der Liste der registrierten Anwendungen entfernen auf S. 36).

6 Bereich **Logdatei**. Ermöglicht die Anzeige von Informationen über Änderungen der Netzzugangsmöglichkeiten von Anwendungen. Die Einstellungen für die Logdatei (s. Logdatei-Parameter einstellen auf S. 52) sowie das Festlegen eines Filters für die Darstellung der Ereignisse

(s. Filter der Ereignisdarstellung einstellen auf S. 54) können in den entsprechenden Bereichen vorgenommen werden.

7 Bereich **Einstellungen**. Ermöglicht das Festlegen von Parametern für die Überwachung der Netzaktivitäten von Anwendungen (s. Überwachungsparameter für Netzaktivitäten einstellen auf S. 46) sowie für die Verfolgung von Änderungen in den Programmen (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48).

Besonderheiten der Arbeit mit „Programmkontrolle“ über eine Terminalsitzung

Der Einsatz von „Programmkontrolle“ auf einem Terminalserver erlaubt es jedem Benutzer, Anwendungen, die in der eigenen Sitzung gestartet wurden, die Arbeit im Netzwerk zu erlauben oder zu verbieten, sowie die Netzaktivitäten von Netzwerkdiensten zu erlauben oder zu blockieren. Bei ausreichendem Umfang der Benutzerrechte (s. Benutzerrechte in ViPNet Programmkontrolle auf S. 13) können außerdem die Einstellungen des Programms für alle Benutzersitzungen geändert werden. Die Arbeit mit „Programmkontrolle“ auf einem Terminalserver hat einige Besonderheiten.

Wenn auf dem Terminalserver mehrere Benutzersitzungen aktiv sind, und einer der Benutzer die Konfiguration des Programms „Programmkontrolle“ (s. Konfigurieren des Programms auf S. 45) durchführt, dann werden die Änderungen in allen Benutzersitzungen übernommen. Die Benutzeroberfläche des Programms „Programmkontrolle“ wird in allen Benutzersitzungen in Übereinstimmung mit den neuen Parametern aktualisiert.

Wenn mehrere Benutzer gleichzeitig die Konfiguration von „Programmkontrolle“ durchführen, werden nur die Änderungen desjenigen Benutzers übernommen, der diese als Erster abspeichert. In den Sitzungen anderer Benutzer wird beim Speicherversuch ein Fenster mit der Meldung eingeblendet, dass die Parameter des Programms bereits von einem anderen Benutzer geändert wurden.

ViPNet Coordinator [Programmkontrolle]

Während Sie die Einstellungen bearbeitet haben, wurden diese von einem anderen Benutzer modifiziert. Die aktualisierten Einstellungen werden jetzt übernommen. Anschließend können Sie mit dem Editieren fortfahren.

OK

Abbildung 4. Meldung über die von einem anderen Benutzer modifizierte Einstellungen

Wenn einer der Benutzer eine Anwendung gestartet hat, die Netzwerkaktivitäten aufweist, dann wird das Fenster, das die Wahl weiterer Schritte bezüglich dieser Anwendung seitens „Programmkontrolle“ ermöglicht, nur in der Sitzung dieses Benutzers eingeblendet.

Wenn in einer der Benutzersitzungen eine Anwendung registriert wurde, dann wird diese Anwendung in der Liste registrierter Anwendungen von „Programmkontrolle“ in allen Benutzersitzungen angezeigt (s. Liste der registrierten Anwendungen anzeigen auf S. 32). Über die Besonderheiten der Registrierung von Netzwerkdiensten s. Abschnitt Konfiguration des Netzzugangs von Netzwerkdiensten auf dem Terminalserver (auf S. 30).

Informationen über den Benutzerwechsel und die Anmeldung in „Programmkontrolle“ im Namen des Administrators über eine Terminalsitzung s. Abschnitte:

- Benutzerwechsel über eine Terminalsitzung (s. Anmeldung in „Programmkontrolle“ als Administrator über eine Terminalsitzung auf S. 40);
- Anmeldung in „Programmkontrolle“ als Administrator über eine Terminalsitzung (auf S. 40).

Betrachten wir als Beispiel die Registrierung einer Anwendung unter Verwendung eines Terminalservers:

1. Auf dem Terminalserver ist ViPNet Software mitsamt „Programmkontrolle“ installiert. Zusätzlich sind folgende Bedingungen erfüllt:
    - Für den Netzwerkknoten ist ein mittlerer Umfang an Rechten definiert (s. Benutzerrechte in ViPNet Programmkontrolle auf S. 13).
    - Benutzer A arbeitet im Netzwerkknotenadministrator-Modus (s. Netzwerkknoten Administrator auf S. 56).
    - In den Einstellungen des Programms ist das Kontrollkästchen **Beim Start von Windows nach Authentisierung in ViPNet automatisch starten** aktiviert.
    - Bei Konfiguration der Sicherheitsrichtlinie wurde die Richtlinie **Benutzer fragen** ausgewählt (s. Richtlinie „Benutzer fragen“ wählen auf S. 28).
2. Benutzer B meldet sich am Terminalserver mit seinem Windows-Benutzerkonto an, um per Fernzugriff zu arbeiten.
3. In der Sitzung des Benutzers B wird automatisch das Programm „Programmkontrolle“ gestartet.
4. Benutzer B startet das Programm „Internet Explorer“ und erhält die Meldung, dass die Anwendung „Internet Explorer“ Netzwerkaktivitäten aufweist. Im Fenster der Meldung muss er eine Aktion auswählen, die von „Programmkontrolle“ im Hinblick auf das Programm „Internet Explorer“ ausgeführt werden soll.
5. Benutzer B erlaubt es der Anwendung, im Netzwerk aktiv zu werden.
6. Die Anwendung wird in „Programmkontrolle“ für die weitere Arbeit im Netzwerk registriert. Die Liste registrierter Anwendungen wird in Sitzungen beider Benutzer aktualisiert (s. Arbeit mit der Liste der Anwendungen, die von „Programmkontrolle“ registriert sind auf S. 32).

Wenn Benutzer B später entscheidet, der Anwendung „Internet Explorer“ die Arbeit im Netz wieder zu verbieten, oder die Anwendung aus der Liste registrierter Anwendungen zu löschen, wird er diese Aktionen nicht durchführen können, da der eingeschränkte Umfang an Rechten eine Änderung dieser Einstellungen nicht erlaubt. In diesem Fall muss sich Benutzer B an Benutzer A wenden, der sich im Programm „Programmkontrolle“ als Administrator des Netzwerkknotens anmelden (s. Anmeldung in „Programmkontrolle“ als Administrator über eine Terminalsitzung auf S. 40) und alle erforderlichen Änderungen vornehmen kann.

Wenn auf dem Terminalserver Netzwerkaktivitäten von Diensten registriert werden, dann wird die Vorgehensweise des Programms „Programmkontrolle“ anders aussehen (s. Konfiguration des Netzzugangs von Netzwerkdiensten auf dem Terminalserver auf S. 30).

2

Schnellstart

Einer Anwendung die Arbeit im Netzwerk erlauben

Sofort nach der Installation beginnt ViPNet „Programmkontrolle“, die Netzwerkaktivitäten der Anwendungen zu überwachen. Standardmäßig ist der Netzzugang für alle Anwendungen erlaubt, deswegen wird bei der ersten erfassten Netzaktivität irgendeiner Anwendung sofort die Meldung eingeblendet, dass die betroffene Anwendung eine Erlaubnis für den Netzzugang hat. Im gleichen Meldungsfenster kann festgelegt werden, welche Aktionen seitens „Programmkontrolle“ bei nachfolgenden Netzwerkaktivitäten der gegebenen Anwendung ausgeführt werden sollen.

Abbildung 5. Fenster der Anfrage um Erlaubnis für den Netzzugang

So erhält ein Programm die Erlaubnis für die Arbeit im Netzwerk:

1. Wählen Sie im Meldungsfenster die Option **Netzzugang erlauben**.
2. Klicken Sie auf **OK**.

Die betroffene Anwendung wird registriert und bekommt dadurch die Erlaubnis, im Netzwerk arbeiten zu können.

Wenn der Netzzugang einer Anwendung bei der nächsten Netzaktivität erlaubt werden soll, gleichzeitig aber erneut eine Meldung erscheinen soll, die das Festlegen weiterer Aktionen seitens „Programmkontrolle“ ermöglicht:

1. Wählen Sie im Meldungsfenster die Option **Beim nächsten Programmstart erneut anfragen**.
2. Klicken Sie auf **OK**.

Dadurch wird für die betroffene Anwendung bei der nächsten Netzaktivität der Netzzugang erlaubt sein, gleichzeitig wird aber erneut ein Meldungsfenster eingeblendet, mit dessen Hilfe festgelegt werden kann, ob das betroffene Programm bei nachfolgenden Netzaktivitäten den Netzzugang erhält oder nicht.

Einer Anwendung die Arbeit im Netzwerk verbieten

Im Meldungsfenster, das standardmäßig bei der ersten Netzaktivität einer Anwendung angezeigt wird, kann dieser Anwendung die Arbeit im Netzwerk verboten werden. Dazu:

1. Wählen Sie im Meldungsfenster die Option **Netzzugang blockieren**.
2. Klicken Sie auf **OK**.

Dadurch wird die betroffene Anwendung registriert und wird für sie der Netzzugang blockiert sein.

Führen Sie einen der folgenden Schritte aus, um einer blockierten Anwendung den Netzzugang zu ermöglichen:

- Entfernen Sie das Programm aus der Liste der registrierten Anwendungen und registrieren Sie es neu (s. Eine Anwendung aus der Liste der registrierten Anwendungen entfernen auf S. 36).
- Ändern Sie den Zugriffsmodus der Anwendung auf das Netzwerk (s. Netzzugang von Anwendungen einstellen auf S. 35).

Anzeige von Meldungen und Anfragen deaktivieren

Führen Sie folgende Schritte aus, um die Anzeige von Meldungen über erlaubte oder blockierte Netzaktivitäten von Anwendungen sowie die Anfragen von Programmen über den Erhalt eines Netzzugangs zu deaktivieren:

1 Wählen Sie im linken Bereich des „Programmkontrolle“ Hauptfensters den Eintrag **Einstellungen**.

2 Wählen Sie in Gruppe **Sicherheitsrichtlinie** in der Dropdownliste **Wenn Netzaktivitäten vorhanden** eine der folgenden Optionen:

   - **Netzzugang erlauben**. Netzaktivität wird für alle nicht registrierte Anwendungen erlaubt sein.
   - **Netzzugang blockieren**. Netzaktivität wird für alle nicht registrierte Anwendungen blockiert sein.

Abbildung 6. Sicherheitsrichtlinie bei Netzaktivitäten von Programmen einstellen

3 Klicken Sie auf **Übernehmen**.

Dadurch wird die in den obigen Schritten festgelegte Aktion automatisch ausgeführt.

Um keine Meldungen von „Programmkontrolle“ mehr zu erhalten, kann die Funktion der Anwendungskontrolle vollständig deaktiviert werden (s. „Programmkontrolle“ ausschalten auf S. 37).

Wie kann der Netzzugang einer nicht registrierten Anwendung ohne vorhergehende Anfrage erlaubt oder blockiert werden

Eine Anwendung gilt als nicht registriert, wenn sie noch nie Netzwerkaktivitäten verursacht hat, oder wenn für sie im Meldungsfenster zum Festlegen der Erlaubnis für die Arbeit im Netzwerk die Option **Beim nächsten Programmstart erneut anfragen**, **Diesmal erlauben** oder **Diesmal blockieren** gewählt wurde. Wenn die Notwendigkeit besteht, Netzzugangsparameter für nicht registrierte Anwendungen festlegen zu müssen, führen Sie folgende Schritte aus:

1. Klicken Sie im Hauptmenü auf **Einstellungen** > **Programm konfigurieren**.
2. In Abhängigkeit von der gewählten Alternative (einer Anwendung die Arbeit im Netzwerk erlauben oder blockieren), wählen Sie den Eintrag **Netzzugang erlauben** oder **Netzzugang blockieren**.
3. Wählen Sie im Fenster **Hinzufügen der Datei zur Liste** die entsprechende Anwendungsdatei mit der Erweiterung .exe aus und klicken Sie auf **Öffnen**.

Als Folge wird in der Tabelle der registrierten Anwendungen das gewählte Programm aufgelistet, mit Status **Verboten** oder **Erlaubt** in der Spalte **Arbeit im Netzwerk**.

Auf diese Weise wird die gewählte Anwendung von „Programmkontrolle“ registriert, um dem Programm bei Nachweis einer Netzaktivität den Netzzugang zu erlauben oder zu verbieten.

3

Kontrolle der Netzaktivitäten von Anwendungen

„Programmkontrolle“ starten und beenden

Bei Netzwerken auf Basis der Software ViPNet Administrator wird das Programm „Programmkontrolle“ im Regelfall gleichzeitig mit der ViPNet Software gestartet, deren Komponente es bildet. Bei Bedarf kann der automatische Start der „Programmkontrolle“ deaktiviert werden (s. Wie kann man den automatischen Start des Programms „Programmkontrolle“ deaktivieren auf S. 26).

Beim Arbeiten mit ViPNet VPN kann der erste Start des Programms Programmkontrolle nur manuell durchgeführt werden. Anschließend kann bei Bedarf der automatische Start des Programms konfiguriert werden.

Um „Programmkontrolle“ manuell zu starten, wählen Sie im Hauptfenster des Programms ViPNet Client oder Coordinator Monitor im Menü **Anwendungen** den Eintrag **Programmkontrolle**. Beim Verwenden der Programme ViPNet Personal Firewall oder ViPNet Office Firewall klicken wählen Sie im Menü **Datei** den Eintrag **Programmkontrolle**.

Führen Sie einen der folgenden Schritte durch, um das Programmfenster von „Programmkontrolle“ auszublenden:

- Klicken Sie in der rechten oberen Fensterecke auf die Schaltfläche **Schließen** .
- Wählen Sie im Hauptmenü **Einstellungen** > **Verstecken** oder **Beenden.**
- Drücken Sie die Tastenkombination **Alt+F4**.

Dadurch wird die Überwachung der Netzaktivitäten von Anwendungen gestoppt.

Zum Ausschalten der Funktion der Anwendungskontrolle siehe Abschnitt „Programmkontrolle“ ausschalten (auf S. 37).

Wie kann man den automatischen Start des Programms „Programmkontrolle“ deaktivieren

Damit das Programm „Programmkontrolle“ nicht beim Start der ViPNet Software gestartet wird, führen Sie folgende Aktionen durch:

1 Wählen Sie den Bereich **Einstellungen** in der Leiste **Programmkontrolle** im Hauptfenster des Programms aus.

2 Deaktivieren Sie das Kontrollkästchen **Immer mit Windows starten**.

3 Klicken Sie auf **Übernehmen**.

  Als Ergebnis wird das Programm „Programmkontrolle“ beim Booten von Windows nicht gestartet. In diesem Fall muss zur Kontrolle der Netzwerkaktivität von Anwendungen die „Programmkontrolle“ manuell gestartet werden (s. „Programmkontrolle“ starten und beenden auf S. 25).

Die „Programmkontrolle“ kann nur zusammen mit der Software gestartet wird, die das Programm enthält. Deswegen, wenn beim Systemstart die ViPNet Software nicht gestartet wird, wird das Programm „Programmkontrolle“ ebenfalls nicht gestartet. Wenn nach dem Start des Betriebssystems die ViPNet Software manuell gestartet wurde, muss die „Programmkontrolle“ auch manuell aufgerufen werden (s. „Programmkontrolle“ starten und beenden auf S. 25).

Anfrage über Arbeit im Netzwerk

Die Hauptbestimmung von „Programmkontrolle“ ist es, Anwendungen zu registrieren, die Netzaktivitäten auf dem Rechner verursachen. Der Benutzer wird gefragt, ob eine Anwendung im Netzwerk arbeiten darf, wenn:

1. Die Anwendung noch nicht von „Programmkontrolle“ registriert wurde.
2. Die Anwendung aus der Liste der registrierten Anwendungen entfernt wurde (s. Eine Anwendung aus der Liste der registrierten Anwendungen entfernen auf S. 36).
3. Die Anwendung in „Programmkontrolle“ bereits registriert ist, sich jedoch bestimmte Eigenschaften dieser Anwendung geändert haben (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48) – es wurde zum Beispiel die Programmversion aktualisiert.

Beim Versuch einer Anwendung, im Netzwerk irgendeine Aktivität auszuführen, wird der Anwendung standardmäßig die Arbeit im Netz erlaubt. Es öffnet sich ein Meldungsfenster, mit dessen Hilfe die Handlungsweise von „Programmkontrolle“ bei nachfolgenden Netzaktivitäten der Anwendung festlegt werden kann.

Der Inhalt der Meldung hängt von der gewählten Sicherheitsrichtlinie ab. Das Programm „Programmkontrolle“ erlaubt dabei, eine der folgenden Einstellungen auszuwählen:

- Netzzugang erlauben.
- Erlaubt nach Benutzeranfrage.
- Benutzer fragen.
- Verboten nach Benutzeranfrage.
- Netzzugang blockieren.

Durch die Wahl der Einstellung **Netzzugang erlauben** oder **Netzzugang blockieren** wird der Zugang der Anwendungen zum Netz ohne weitere Meldungen (s. Anzeige von Meldungen und Anfragen deaktivieren auf S. 22) erlaubt oder blockiert werden.

Richtlinie „Erlaubt nach Benutzeranfrage“ wählen

Wenn beim Festlegen der Sicherheitsrichtlinie die Standardeinstellungen beibehalten wurden (das heißt, dass die Richtlinie **Erlaubt nach Benutzeranfrage** aktiv ist), wird für die betroffene Anwendung die Arbeit im Netzwerk erlaubt sein. Es muss jedoch festgelegt werden, welche Aktionen von „Programmkontrolle“ bei der nächsten Netzaktivität dieser Anwendung ausgeführt werden sollen. Im nicht-interaktiven Modus (s. Nicht-interaktiver Modus auf S. 56) wird die Arbeit der Anwendung im Netzwerk erlaubt.

Um der Anwendung den Netzzugang zu erlauben, wenn mit der Richtlinie **Erlaubt nach Benutzeranfrage** gearbeitet wird, führen Sie die im Abschnitt Einer Anwendung die Arbeit im Netzwerk erlauben (auf S. 19) aufgeführten Schritte durch.

Um der Anwendung den Netzzugang zu blockieren, wenn mit der Richtlinie **Erlaubt nach Benutzeranfrage** gearbeitet wird, führen Sie die im Abschnitt Einer Anwendung die Arbeit im Netzwerk verbieten (auf S. 21) aufgeführten Schritte durch.

Richtlinie „Benutzer fragen" wählen

Wenn beim Festlegen der Sicherheitsrichtlinie (s. Überwachungsparameter für Netzaktivitäten einstellen auf S. 46) die Richtlinie **Benutzer fragen** ausgewählt wurde, werden bei der nächsten Netzaktivität einer Anwendung keine Handlungen gesetzt, bis konkrete Anweisungen des Benutzers erfolgen.

Abbildung 7. Anfragefenster bei Wahl der Einstellung „Benutzer fragen"

Tipp. Um im Meldungsfenster die Gruppe **Über das Programm** ein- oder auszublenden, klicken Sie auf die Schaltfläche **Über**.

So wird einer Anwendung der Netzzugang erlaubt, wenn mit der Richtlinie **Benutzer fragen** gearbeitet wird:

1 Wählen Sie im Anfragefenster:

  - **Netzzugang erlauben**. Die Anwendung wird registriert und die Netzaktivität wird für die gegebene Anwendung erlaubt.
  - **Diesmal erlauben**. Die Netzwerkarbeit der gegebenen Anwendung wird für die aktuelle Sitzung erlaubt, bei der nächsten Netzaktivität des Programms wird jedoch die gleiche Anfrage erneut eingeblendet.

2 Klicken Sie auf **OK**.

So wird einer Anwendung der Netzzugang blockiert, wenn mit der Richtlinie **Benutzer fragen** gearbeitet wird:

1. Wählen Sie im Anfragefenster:
   - **Netzzugang blockieren**. Die Anwendung wird registriert und die Netzaktivität der Anwendung wird verboten, das heißt, jeder Versuch, auf das Netzwerk zuzugreifen, wird blockiert.
   - **Diesmal blockieren**. Die Netzwerkarbeit der gegebenen Anwendung wird für die aktuelle Sitzung verboten, bei der nächsten Netzaktivität des Programms wird jedoch die gleiche Anfrage erneut eingeblendet.
2. Klicken Sie auf **OK**.

Wenn die Richtlinie **Benutzer fragen** ausgewählt wurde und eine Anwendung Netzwerkaktivitäten aufweist, zum gegenwärtigen Zeitpunkt aber keine Möglichkeit besteht, die passende Aktion im Meldungsfenster festzulegen, dann wird „Programmkontrolle" die Verarbeitung von Anwendungsanfragen über die Arbeit im Netzwerk im nicht-interaktiven Modus (s. Nicht-interaktiver Modus auf S. 56) durchführen. Details über den nicht-interaktiven Modus bei Verarbeitung von Anfragen s. Abschnitt Verarbeitung von Anfragen der Anwendungen über Netzwerkaktivitäten im nicht-interaktiven Modus (auf S. 50).

Richtlinie „Verboten nach Benutzeranfrage" wählen

Wenn beim Festlegen der Sicherheitsrichtlinie die Richtlinie **Verboten nach Benutzeranfrage** ausgewählt wurde, wird für die betroffene Anwendung die Arbeit im Netzwerk verboten sein. Es muss jedoch festgelegt werden, welche Schritte seitens „Programmkontrolle" bei der nächsten Netzaktivität dieser Anwendung ausgeführt werden sollen.

Abbildung 8. Anfragefenster bei Wahl der Einstellung „Verboten nach Benutzeranfrage"

So wird einer Anwendung der Netzzugang erlaubt, wenn mit der Richtlinie **Verboten nach Benutzeranfrage** gearbeitet wird:

1. Wählen Sie im Anfragefenster:
   - **Netzzugang erlauben**, um die Arbeit der gegebenen Anwendung im Netzwerk immer zu ermöglichen, ohne dass Anfragen um Erlaubnis bei jedem Zugangsversuch gesendet werden.
   - **Beim nächsten Programmstart erneut anfragen**, um die Arbeit der gegebenen Anwendung im Netzwerk dieses Mal zu erlauben, aber bei der nächsten Netzaktivität erneut die Anfrage einzublenden, mit deren Hilfe die weitere Handlungsweise von „Programmkontrolle" festlegt werden kann.
2. Klicken Sie auf **OK**.

So wird einer Anwendung der Netzzugang blockiert, wenn mit der Richtlinie **Verboten nach Benutzeranfrage** gearbeitet wird:

1. Wählen Sie im Anfragefenster die Option **Netzzugang blockieren**, um die Arbeit der gegebenen Anwendung im Netzwerk zu verbieten, ohne dass Anfragen um Erlaubnis bei jedem weiteren Zugangsversuch gesendet werden.
2. Klicken Sie auf **OK**.

Konfiguration des Netzzugangs von Netzwerkdiensten auf dem Terminalserver

Wenn ein Netzwerkdienst Netzaktivitäten auf dem Terminalserver aufweist, wird in der Sitzung des Benutzers, der zu diesem Zeitpunkt auf dem Terminalserver arbeitet, ein Fenster mit der entsprechenden Meldung angezeigt, in welchem weitere Schritte seitens „Programmkontrolle" im Hinblick auf diesen Dienst festgelegt werden können. Dieses Meldungsfenster kann nur an einen Benutzer gerichtet werden. Wenn mehrere Benutzersitzungen auf dem Terminalserver aktiv sind, wird das Fenster unter Beachtung folgender Prioritäten nur in einer der Sitzungen eingeblendet:

1. Benutzer, der über Administratorrechte für den ViPNet Netzwerkknoten verfügt und lokal auf dem Server arbeitet;
2. Benutzer, der über Administratorrechte für den ViPNet Netzwerkknoten verfügt und remote auf dem Server arbeitet;
3. Benutzer, der über keine Administratorrechte für den ViPNet Netzwerkknoten verfügt und lokal auf dem Server arbeitet;
4. Benutzer, der über keine Administratorrechte für den ViPNet Netzwerkknoten verfügt und remote auf dem Server arbeitet.

Beispiel:

1. Auf dem Terminalserver sind zwei Benutzersitzungen gestartet:
   - Benutzer A arbeitet lokal und besitzt keine Administratorrechte;

- Benutzer B arbeitet remote als Administrator eines ViPNet Netzwerkknotens.

2. Auf dem Terminalserver versucht der Netzwerkdienst BranchCache, einen Zugang zum Netz zu erhalten.
3. Das Fenster mit der Meldung über die Netzwerkaktivitäten des Dienstes wird an Benutzer B gerichtet, der einen der vorgeschlagenen Schritte wählen darf.
4. „Programmkontrolle“ führt die gewählte Aktion im Hinblick auf den gegebenen Dienst durch.
5. Wenn der Dienst mit Erlaubnis oder Verbot des Netzwerkzugangs registriert wird (s. Schnellstart auf S. 18), dann wird er in den Listen registrierter Anwendungen beider Benutzer angezeigt.

Arbeit mit der Liste der Anwendungen, die von „Programmkontrolle“ registriert sind

Liste der registrierten Anwendungen anzeigen

Das Programm ViPNet „Programmkontrolle“ ermöglicht es, Informationen über registrierte Anwendungen anzuzeigen, denen die Arbeit im Netzwerk erlaubt oder verboten wurde. Wählen Sie dazu im Hauptfenster von „Programmkontrolle“ in der Navigationsleiste den Bereich **Registrierte Anwendungen**.

Abbildung 9. Einstellungen der registrierten Anwendungen ansehen

In der Übersicht werden folgende Informationen über registrierte Anwendungen in Form einer Tabelle angezeigt:

1. In der Spalte **Arbeit im Netzwerk** wird angegeben, ob einer Anwendung die Arbeit im Netzwerk erlaubt oder verboten ist. Bei der Arbeit im Netzwerk sind folgende Optionen möglich:
    - **Erlaubt**, falls für die Anwendung die Arbeit im Netzwerk erlaubt ist.
    - **Verboten**, falls für die Anwendung die Arbeit im Netzwerk verboten ist.
    - **Erlaubt**, falls für die ViPNet Anwendung die Arbeit im Netzwerk erlaubt ist.
    - **Verboten**, falls für die ViPNet Anwendung die Arbeit im Netzwerk verboten ist.

2 In der Spalte **Programm** werden die Namen der registrierten Anwendungen aufgelistet.

3 In der Spalte **Programmdatei** wird standardmäßig der Pfad zur ausführbaren Datei angezeigt. Wenn in dieser Spalte nur der Name der ausführbaren Datei angezeigt werden soll:

- Wählen Sie im Programmfenster von „Programmkontrolle" im linken Bereich den Eintrag **Einstellungen**.
- Deaktivieren Sie im Anzeigebereich das Kontrollkästchen **Vollständigen Dateipfad anzeigen**.

Abbildung 10. Anzeige für Namen und Pfad der Anwendungsdatei einstellen

4 In der Spalte **Registrierung** werden Datum und Uhrzeit des Beginns der Überwachung von Netzwerkaktivitäten einer Anwendung seitens „Programmkontrolle" angegeben.

5 In der Spalte **Registrierungsweise** wird eine der folgenden Registrierungsarten einer Anwendung aufgelistet:

- **Registriert vom Benutzer**, wenn beim Einstellen der Sicherheitsrichtlinie die Richtlinie **Benutzer fragen** (s. Richtlinie „Benutzer fragen" wählen auf S. 28) gewählt wurde oder die Anwendung in der Liste der registrierten Anwendungen manuell hinzugefügt wurde (s. Wie kann der Netzzugang einer nicht registrierten Anwendung ohne vorhergehende Anfrage erlaubt oder blockiert werden auf S. 23).
- **Automatische Registrierung**, wenn beim Einstellen der Sicherheitsrichtlinie eine andere Richtlinie als **Benutzer fragen** gewählt wurde (s. Anfrage über Arbeit im Netzwerk auf S. 27).
- **Registrierung der ViPNet Anwendung**, wenn die registrierte Anwendung ein Bestandteil des Softwarepakets von ViPNet ist.
- **Programmänderung auf Benutzeranfrage**, wenn beim Festlegen der Parameter für die Überwachung von Änderungen registrierter Anwendungen die Richtlinie **Benutzer fragen** gewählt wurde (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48).
- **Automatische Registrierung der Programmänderung**, wenn beim Festlegen der Parameter für die Überwachung von Änderungen registrierter Anwendungen eine andere Richtlinie als **Benutzer fragen** gewählt wurde (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48).

- **ViPNet Programm Update**, wenn in einer registrierten Anwendung, die Bestandteil des ViPNet Softwarepakets ist, eine Änderung (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48) festgestellt wurde.

6 In der Spalte **Programmänderung** werden Datum und Uhrzeit der letzten Änderung einer Anwendung angezeigt (s. Parameter für die Überwachung von Programmänderungen einstellen auf S. 48). Wenn sich die Anwendung nicht geändert hat, bleibt das Feld leer.

Um den Umfang der im Bereich **Registrierte Anwendungen** aufgelisteten Informationen zu regeln, klicken Sie mit der rechten Maustaste auf die Überschrift einer beliebigen Spalte und aktivieren oder deaktivieren Sie die benötigten Kontrollkästchen.

So zeigen Sie die Eigenschaften registrierter Anwendungen in einem separaten Fenster an:

1 Klicken Sie im Bereich **Registrierte Anwendungen** mit der rechten Maustaste in die Zeile der Anwendung, für die Sie die Eigenschaften anzeigen möchten.

2 Klicken Sie auf **Eigenschaften**.

Dadurch können die allgemeinen Eigenschaften der Anwendung sowie Details über ihre Registrierung in einem separaten Fenster angezeigt werden. Das Eigenschaftenfenster des Host Process enthält neben allgemeinen Informationen auch eine Liste von Diensten, die in diesem Prozess aktiv sind, sowie allgemeine Daten über diese.

Eigenschaften des Programms ViPNet Monitor

Eigenschaften des Host Process Svchost.exe

Abbildung 11. Fenster der Programmeigenschaften

Netzzugang von Anwendungen einstellen

Wenn die Notwendigkeit entsteht, vorhandene Einstellungen für registrierte Anwendungen (das heißt für Anwendungen, für die im Anfragefenster **Netzzugang erlauben** oder **Netzzugang blockieren** gewählt wurde) zu ändern:

1. Wählen Sie im Hauptfenster von "Programmkontrolle" (s. „Programmkontrolle" starten und beenden auf S. 25) in der Leiste **Programmkontrolle** den Eintrag **Registrierte Anwendungen**.
2. Klicken Sie in der Tabelle mit der rechten Maustaste in die Zeile der Anwendung, für die die Einstellungen geändert werden sollen.

   Abbildung 12. Tabelle der registrierten Anwendungen

3. Wählen Sie die benötigte Einstellung:
   - Wenn die Arbeit im Netzwerk für die gegebene Anwendung erlaubt war, wird der Vorschlag angezeigt, den Netzzugang zu blockieren.
   - Wenn die Arbeit im Netzwerk für die gegebene Anwendung verboten war, wird der Vorschlag angezeigt, den Netzzugang zu erlauben.
   - Wenn bei der nächsten Netzwerkaktivität der Anwendung eine Anfrage um Erlaubnis für den Netzzugriff erscheinen soll, wählen Sie **Von der Liste löschen**. Weitere Informationen finden Sie im Abschnitt Eine Anwendung aus der Liste der registrierten Anwendungen entfernen (auf S. 36).
4. In der Tabelle der registrierten Anwendungen ändert sich in Spalte **Arbeit im Netzwerk** der Status der Anwendung (wenn die Arbeit im Netzwerk erlaubt oder blockiert wurde), oder die Anwendung scheint in der Liste nicht mehr auf (wenn das Programm aus der Liste gelöscht wurde).

Wenn die Notwendigkeit besteht, Einstellungen für Anwendungen vorzunehmen, die nicht in der Liste sind, führen Sie die Registrierung der Anwendung manuell durch (s. Wie kann der Netzzugang einer nicht registrierten Anwendung ohne vorhergehende Anfrage erlaubt oder blockiert werden auf S. 23).

Eine Anwendung aus der Liste der registrierten Anwendungen entfernen

Bei der Arbeit mit „Programmkontrolle“ kann die Notwendigkeit entstehen, eine Anwendung, der die Netzaktivität bereits erlaubt oder blockiert wurde, bei jedem weiteren Versuch, im Netzwerk zu arbeiten, wieder um Erlaubnis anfragen zu lassen. Dafür müssen die Anwendung aus der Liste der registrierten Anwendungen entfernt sowie einige neue Parameter eingestellt werden.

So entfernen Sie eine Anwendung aus der Liste der registrierten Anwendungen:

1. Wählen Sie im Programmfenster von „Programmkontrolle“ in der linken Leiste den Eintrag **Registrierte Anwendungen**.
2. Klicken Sie in der Tabelle der registrierten Anwendungen mit der rechten Maustaste in die Zeile der Anwendung, für die der Eintrag entfernt werden soll.
3. Wählen Sie **Von der Liste löschen**.

Dadurch wird die entfernte Anwendung de-registriert. Das bedeutet, dass bei der ersten Netzaktivität eine Anfrage um die Einstellung neuer Parameter für diese Anwendung angezeigt wird. Eine Neuregistrierung der betroffenen Anwendung kann auch manuell erfolgen (s. Wie kann der Netzzugang einer nicht registrierten Anwendung ohne vorhergehende Anfrage erlaubt oder blockiert werden auf S. 23).

„Programmkontrolle“ ausschalten

Hinweis. Hinweis. Standardmäßig ist die Kontrolle der Netzaktivitäten von Anwendungen eingeschaltet, deswegen beginnt das Modul sofort beim Start der ViPNet Software, deren Komponente „Programmkontrolle bildet, die Netzwerkaktivitäten von Anwendungen zu überwachen.

Das Ausschalten der Kontrolle von Netzwerkaktivitäten von Anwendungen führt zu einem Stopp der Überwachung von Anwendungen, die versuchen, auf das Netzwerk zuzugreifen. Das Ausschalten der Kontrolle von Netzaktivitäten führt einerseits zu einer deutlichen Verringerung des Schutzumfangs für Ihren Rechner und kann es Übeltätern ermöglichen, Zugang zu persönlichen Daten zu bekommen, die auf Ihrem Rechner gespeichert sind. Andererseits beseitigt das Ausschalten mögliche Probleme, die durch Konflikte von „Programmkontrolle“ mit anderen Programmen, die den Netzzugang für eine korrekte Funktionsweise brauchen, verursacht wurden. „Programmkontrolle“ ist kompatibel zur Mehrzahl von Anwendungen, die einen Netzzugang erfordern. Beim Auftauchen von irgendwelchen Unregelmäßigkeiten kann das Abschalten der Überwachung von Netzaktivitäten bei der Problemdiagnose einzelner Anwendungen von Drittherstellern hilfreich sein.

Achtung! Für die Gewährleistung der Sicherheit Ihres Rechners wird nachdrücklich empfohlen, das Programm „Programmkontrolle zu aktivieren. Vergessen Sie nicht, die Kontrolle der Netzwerkaktivitäten von Anwendungen wieder zu aktivieren, sobald die Notwendigkeit für das Abschalten wegfällt. Dazu wählen Sie **Einstellungen** > **Programmkontrolle aktivieren**.

Um die Kontrolle der Netzaktivitäten auszuschalten, wählen Sie im Hauptfenster von „Programmkontrolle“ den Menüpunkt **Einstellungen** > **Programmkontrolle deaktivieren**.

Benutzerwechsel in „Programmkontrolle“

Das Programm „Programmkontrolle“ als eine Komponente der Software ViPNet Client und Coordinator erlaubt einen Wechsel des Benutzers. Dank dieser Funktionalität können unterschiedliche ViPNet Benutzer mit „Programmkontrolle“ arbeiten, wobei jeder von ihnen mit seinen eigenen Einstellungen und seiner eigenen Liste der registrierten Anwendungen arbeitet.

Auf einem Rechner, auf dem die Software ViPNet Client und Coordinator installiert ist, können mehrere Benutzer arbeiten. Die Möglichkeit zum Benutzerwechsel erlaubt es jedem Benutzer, in „Programmkontrolle“ unter seinem eigenen Benutzerkonto einzusteigen, ohne die Arbeit mit ViPNet Software zu unterbrechen. So führen Sie einen Benutzerwechsel in „Programmkontrolle“ durch:

1 Wählen Sie im Menü **Einstellungen** den Eintrag **Benutzer wechseln**.

2 Geben Sie das Passwort ein und klicken Sie auf **OK**.

Hinweis. Der Wechsel des Benutzers in einer Komponente des Programmpakets ViPNet bewirkt nicht den Benutzerwechsel in allen anderen Komponenten der Software. Zum Beispiel führt ein Wechsel des Benutzers in ViPNet Monitor nicht zum Wechsel des Benutzers in „Programmkontrolle und umgekehrt.

Dadurch werden im Modul „Programmkontrolle“ die Einstellungen und Daten von registrierten Anwendungen des neuen Benutzers angezeigt.

Benutzerwechsel über eine Terminalsitzung

Ein Benutzerwechsel kann auch über die Terminalsitzung durchgeführt werden. Wenn zum Beispiel auf dem Terminalserver ein anderer Benutzer aktiv war und in „Programmkontrolle“ seine Änderungen in den Einstellungen hinterlassen hat, erlaubt es der Benutzerwechsel, sich im Programm unter dem eigenen Konto anzumelden und mit den eigenen Einstellungen zu arbeiten. Dazu:

1 Wählen Sie in der eigenen Sitzung im Menü **Optionen** den Punkt **Benutzer wechseln**.

2 Geben Sie das Passwort ein und klicken Sie auf **OK**.

Dadurch werden in „Programmkontrolle“ die Einstellungen des neuen Benutzers übernommen. Die Benutzerschnittstelle des Programms wird in allen Benutzersitzungen auf diesem Terminalserver aktualisiert.

Wenn auf dem Terminalserver mehrere Anwender gleichzeitig versuchen, in „Programmkontrolle“ den aktuellen Benutzer zu wechseln, kann nur der Benutzer, der als Erster den Befehl **Benutzer wechseln** ausgeführt hat, den Vorgang erfolgreich abschließen. In den Sitzungen anderer Benutzer wird die

Meldung eingeblendet, dass der Benutzerwechsel in „Programmkontrolle“ bereits von einem anderen Benutzer ausgeführt wird, und der Vorgang später wiederholt werden sollte.

Abbildung 13. Meldung über den berets durchführenden Vorgang des Benutzerwechsels

Wenn auf dem Terminalserver einer der Benutzer die Konfiguration des Programms „Programmkontrolle“ durchführt, und ein anderer Benutzer zum gleichen Zeitpunkt versucht, den Befehl **Benutzer wechseln** auszuführen, dann erhält der zweite Benutzer eine Meldung darüber, dass in einer anderen Sitzung Änderungen an den Einstellungen des Programms „Programmkontrolle“ vorgenommen werden und ein Benutzerwechsel zum gegenwärtigen Zeitpunkt nicht möglich ist. Der Vorgang des Benutzerwechsels kann zu einem späteren Zeitpunkt durchgeführt werden.

Anmeldung als Administrator in „Programmkontrolle“

Der Administrator des ViPNet Netzwerks kann auf jedem Netzwerkknoten unter seinem eigenen Namen in „Programmkontrolle“ einsteigen und Einstellungen vornehmen, die für andere Benutzer aus Mangel an Benutzerrechten nicht verfügbar sind.

Zum Einsteigen als Administrator:

1. Wählen Sie im Menü **Optionen** den Eintrag **Administrator-Login**.
2. Geben Sie das Passwort des ViPNet Netzwerkknotenadministrators ein und klicken auf **OK**.

Als Ergebnis werden alle Einstellungen des Programms „Programmkontrolle für das Editieren verfügbar

Anmeldung in „Programmkontrolle“ als Administrator über eine Terminalsitzung

Auf dem Terminalserver kann die Anmeldung in „Programmkontrolle“ im Namen des Administrators durchgeführt werden, um Parameter einzustellen, die wegen fehlender Benutzerrechte nicht verfügbar waren.

Wenn sich ein Benutzer auf dem Terminalserver in einer der Benutzersitzungen in „Programmkontrolle“ als Administrator anmeldet, dann ändert sich der Umfang der Benutzerrechte in den anderen Sitzungen nicht. Die im Namen des Administrators geänderten Einstellungen werden aber von „Programmkontrolle“ in allen Sitzungen übernommen.

4

Statistik und Logdatei einsehen

Statistik einsehen

Informationen über registrierte Anwendungen können in folgender Form angezeigt werden:

- Statistik (das heißt die Anzahl der registrierten Anwendungen);
- detaillierte Informationen über Anwendungen und ihre Einstellungen für den Netzzugang.

So zeigen Sie die Statistik an, wählen Sie im Hauptfenster des Programms in der Leiste **Programmkontrolle** den Eintrag **Programmkontrolle**.

Abbildung 14. Statistik der registrierten Anwendungen anzeigen

Im Bereich **Programmkontrolle** können folgende Daten eingesehen werden:

- Die Gesamtanzahl der vom Programm registrierten Anwendungen.
- Die Anzahl der Anwendungen, für die der Netzzugang erlaubt ist.
- Die Anzahl der Anwendungen, für die der Netzzugang blockiert ist.

Logdatei einsehen

Einträge der Logdatei sind in Form einer Tabelle dargestellt, welche Informationen über die Änderung des Anwendungsstatus enthält. Auf diese Weise ermöglicht die Logdatei die Kontrolle darüber, welche Aktionen wann an den Anwendungen vorgenommen wurden. Die Art und der Umfang der Informationen, die auf dem Bildschirm dargestellt und in der Logdatei gespeichert werden sollen in den Logdatei-Einstellungen (s. Logdatei-Parameter einstellen auf S. 52) sowie in den Filter-Einstellungen für die Ereignisdarstellung (s. Filter der Ereignisdarstellung einstellen auf S. 54) festgelegt werden.

Zum Anzeigen der Logdatei:

1 Wählen Sie im Hauptfenster von „Programmkontrolle“ in der linken Leiste den Abschnitt **Logdatei**.

2 Klicken Sie im Fensterbereich **Logdatei** auf **Aktualisieren**.

3 Dadurch wird in diesem Fensterbereich eine Liste der Ereignisse eingeblendet.

Abbildung 15. Logdatei

Die Logdatei kann auch in anderen Programmen angezeigt werden:

- Zum Anzeigen der Logdatei im HTML-Format klicken Sie auf **Als Webseite anzeigen**.
- Zum Anzeigen der Logdatei in Form einer Microsoft Excel-Tabelle klicken Sie auf **In Microsoft Excel anzeigen**.

Die Anzeige der Logdatei in anderen Formaten ermöglicht es, die Logdatei für eine mögliche weitere Verwendung zu modifizieren, zu speichern und auszudrucken.

In der Logdatei des Programms „Programmkontrolle werden insgesamt 14 Ereignisarten registriert. Alle möglichen Ereignisarten sind in der Tabelle unten dargestellt.

Tabelle 4. Ereignistypen, die in der Logdatei von „Programmkontrolle angezeigt werden

Ereigniscode	Ereignisbeschreibung
1	Übertragung blockiert
2	Übertragung erlaubt

Ereigniscode	Ereignisbeschreibung
3	Netzzugang wegen Änderung des Programms blockiert
4	Netzzugang nach Änderung des Programms erlaubt
5	Hinzugefügt in der Liste der erlaubten Anwendungen
6	Hinzugefügt in der Liste der verbotenen Anwendungen
7	Netzzugang blockiert
8	Netzzugang erlaubt
9	Öffnen des Ports für Datenempfang blockiert
10	Öffnen des Ports für Datenempfang erlaubt
11	Herstellung einer Verbindung blockiert
12	Herstellung einer Verbindung erlaubt
13	Gelöscht aus der Liste der erlaubten Anwendungen
14	Gelöscht aus der Liste der verbotenen Anwendungen

5

Konfigurieren des Programms

Überwachungsparameter für Netzaktivitäten einstellen

Die Einstellung der Parameter für die Überwachung von Netzaktivitäten ermöglicht es, Aktionen zu bestimmen, die von „Programmkontrolle" im Fall der Netzaktivität irgendeiner Anwendung ausgeführt werden. Zum Einstellen dieser Parameter:

1. Klicken Sie im Programmfenster in der linken Übersicht auf den Abschnitt **Einstellungen**.
2. Wählen Sie in Gruppe **Sicherheitsrichtlinie** in der Dropdownliste **Wenn Netzaktivitäten vorhanden** einen der Einträge (s. Anfrage über Arbeit im Netzwerk auf S. 27) aus.

Abbildung 16. Überwachungsparameter für Netzaktivitäten einstellen

3. Standardmäßig sind Systemverbindungen erlaubt. Aus Sicherheitsgründen kann, wenn nötig, das Kontrollkästchen **Systemverbindungen erlauben** wieder deaktiviert werden, um mögliche von einem Übeltäter im Namen des Systems aufgebaute Verbindungen zu blockieren.

Achtung! Das Blockieren von Systemverbindungen kann unerwünschte Folgen nach sich ziehen. Diese Möglichkeit sollte nur von fortgeschrittenen Windows-Benutzern in Anspruch genommen werden.

4. Damit Netzaktivitäten von Anwendungen erlaubt werden, die von einem Netzwerkobjekt gestartet sind, stellen Sie sicher, dass das Kontrollkästchen **Verbindungen mit Anwendungen erlauben, die vom Remote-Server gestartet werden** aktiviert ist. Die Verarbeitung der Anfragen von Anwendungen, die remote gestartet wurden, erfolgt folgenderweise:
   - Wenn das Kontrollkästchen aktiviert ist, und die Anwendung für die Arbeit im Netzwerk nicht registriert ist, oder wenn die Anwendung registriert ist und gleichzeitig die Arbeit im Netzwerk erlaubt ist, wird dieser Anwendung der Netzwerkzugang erlaubt.

- Wenn das Kontrollkästchen aktiviert, und die Anwendung registriert ist, jedoch die Arbeit im Netzwerk für diese Anwendung verboten ist, wird der Netzwerkzugang für diese Anwendung blockiert.
- Wenn das Kontrollkästchen deaktiviert ist, wird die Anfrage der Anwendung genauso verarbeitet, wie die Anfrage einer Anwendung, die lokal gestartet wurde.

5. Klicken Sie auf **Übernehmen**.

Dadurch wird bei jeder Feststellung einer Netzaktivität die gewählte Aktion automatisch ausgeführt.

Parameter für die Überwachung von Programmänderungen einstellen

Nachdem eine Anwendung in „Programmkontrolle“ registriert wurde, können an dieser Anwendung irgendwelche Änderungen auftreten. Diese Änderungen können einerseits ein Ergebnis des planmäßigen Einsatzes der Anwendung sein, wie zum Beispiel eine Aktualisierung der Softwareversion oder eine Erweiterung um neue Funktionen. Andererseits können registrierte Anwendungen von schädlicher Software modifiziert werden, wobei in diesem Fall der Netzzugang für die entsprechende Anwendung gesperrt werden sollte.

Die Einstellung der Parameter für die Überwachung der Programmänderungen ermöglicht die Entscheidung, ob „Programmkontrolle“ die Änderungen in den Programmen kontrollieren soll, und wenn ja - welche genau, sowie welche Aktionen gesetzt werden sollen, wenn Veränderungen festgestellt werden.

Zum Einstellen der Überwachungsparameter für Änderungen in den Anwendungen:

1. Wählen Sie im Programmfenster in der linken Übersicht den Abschnitt **Einstellungen**.
2. Wählen Sie im Bereich **Einstellungen** in Gruppe **Sicherheitsrichtlinie** in der Dropdownliste **Änderungen in den Programmen verfolgen** einen der folgenden Einträge aus:
   - **Nicht verfolgen**, wenn Änderungen in den Anwendungen keinen Einfluss auf die Entscheidung über die Arbeit im Netzwerk haben sollen.
   - **Anhand der Prüfsumme der Programmdatei** (das heißt, anhand eines Werts, der die Integrität und Authentizität der übertragenen Daten bestätigt), wenn es nötig ist, dass die Programmänderungen kontrolliert werden, und dementsprechend bei einer Änderung der Prüfsumme der Anwendungsdatei eine erneute Registrierung der Anwendung erforderlich wird.
   - **Anhand der Dateigröße**, damit bei der Änderung der Größe der ausführbaren Anwendungsdatei eine erneute Registrierung der Anwendung angefordert wird.

Abbildung 17. Parameter für die Überwachung von Programmänderungen einstellen

3 Wählen Sie in Gruppe **Sicherheitsrichtlinie** in der Dropdownliste **Wenn das Programm geändert wurde** einen der Einträge aus. Hier wird die gleiche Liste an Optionen angeboten wie in der Dropdownliste **Wenn Netzaktivitäten vorhanden** (s. Überwachungsparameter für Netzaktivitäten einstellen auf S. 46).

4 Klicken Sie auf **Übernehmen**.

Dadurch werden bei der nächsten Netzaktivität des geänderten Programms die gewählten Aktionen ausgeführt.

Verarbeitung von Anfragen der Anwendungen über Netzwerkaktivitäten im nicht-interaktiven Modus

Die Verarbeitung einer Anwendungsanfrage über die Arbeit im Netzwerk im nicht-interaktiven Modus erlaubt es dem Benutzer, dieser Anwendung die Netzwerkaktivität dann zu erlauben oder zu blockieren, wenn eine der interaktiven Sicherheitsrichtlinien (s. Interaktive Sicherheitsrichtlinie auf S. 56) ausgewählt ist, und der Benutzer zum gegenwärtigen Zeitpunkt keine Möglichkeit hat, die passende Aktion des Programms ViPNet Programmkontrolle im Meldungsfenster über Netzwerkaktivitäten von Anwendungen zu bestimmen. Die Verarbeitung von Anfragen im nicht-interaktiven Modus wird in folgenden Fällen veranlasst:

- die aktuelle Sitzung des Benutzers ist blockiert;
- das Programm „Programmkontrolle“ ist nicht gestartet;
- beim Start des Betriebssystems, wenn noch keine Anmeldung in ViPNet Software, die als Komponente auch „Programmkontrolle“ umfasst, durchgeführt wurde.

Das Erlauben oder Blockieren der Netzaktivitäten von Anwendungen im nicht-interaktiven Modus kann zum Beispiel dann erforderlich sein, wenn Dienste des Betriebssystems geladen werden. Die Überwachung der Netzaktivitäten von Anwendungen ist bereits gestartet, die Anmeldung in ViPNet Software, die als Komponente auch „Programmkontrolle“ umfasst, wurde jedoch noch nicht durchgeführt. Der rechtzeitige Zugang der Dienste zum Netzwerk sichert aber den problemlosen Start des Betriebssystems.

Wenn die Richtlinie **Erlaubt nach Benutzeranfrage** oder **Verboten nach Benutzeranfrage** gewählt wurde, dann wird im nicht-interaktiven Modus die Arbeit der Anwendung im Netzwerk dementsprechend erlaubt oder blockiert (genauso wie im Normalbetrieb). Im interaktiven Modus wird ein Fenster mit der Meldung über Netzwerkaktivitäten der Anwendung eingeblendet, in welchem der Benutzer die weiteren Schritte des Programms „Programmkontrolle“ festlegen kann.

Wenn die Richtlinie **Benutzer fragen** ausgewählt wurde, dann wird im nicht-interaktiven Modus die Arbeit der Anwendung im Netzwerk standardmäßig erlaubt. Führen Sie folgende Schritte aus, um die Netzaktivitäten von Anwendungen bei Verarbeitung der Anfragen im nicht-interaktiven Modus zu blockieren:

1. Wählen Sie im Programmfenster von „Programmkontrolle“ in der Navigationsleiste den Bereich **Einstellungen**.
2. Deaktivieren Sie im Anzeigebereich in Gruppe **Sicherheitsrichtlinie** die Kontrollkästchen **Arbeit im Netzwerk im nicht-interaktiven Modus erlauben**.

Abbildung 18. Verarbeitung von Anfragen der Anwendungen über Netzwerkaktivitäten im nicht-interaktiven Modus

3 Klicken Sie auf **Übernehmen**.

Bei Verarbeitung von Anwendungsanfragen im nicht-interaktiven Modus wird dadurch die Arbeit dieser Anwendungen im Netzwerk standardmäßig verboten.

Logdatei-Parameter einstellen

Das Programm ViPNet Programmkontrolle erlaubt es, die maximale Größe der Logdatei (s. Logdatei einsehen auf S. 43), die zu erfassenden Ereignistypen sowie die Parameter der Logdatei-Aktualisierung einzustellen. Zum Einstellen der Logdatei-Parameter:

1 Klappen Sie im Hauptfenster des Programms den Eintrag **Logdatei** auf.

2 Wählen Sie in der linken Leiste den Bereich **Logdatei-Einstellungen**.

3 Zum Einstellen der maximalen Größe der Logdatei geben Sie im entsprechenden Feld den benötigten Wert (in MB) an. Beim Erreichen der maximalen Größe der Logdatei werden alle Einträge in chronologischer Reihenfolge in das Logdatei-Archiv verschoben. Der Wert 0 bedeutet, dass eine Beschränkung der Logdatei-Größe fehlt.

Abbildung 19. Logdatei-Parameter einstellen

4 Zum Einstellen der maximalen Größe des Archivs geben Sie im entsprechenden Feld den benötigten Wert (in MB) an. Beim Erreichen der maximalen Größe der Archivdatei werden die ältesten Einträge gelöscht. Der Wert 0 bedeutet, dass eine Beschränkung der Größe des Archivs fehlt.

5 Wählen Sie in Gruppe **Ereignisregistrierung** in der Liste **Ereignisse registrieren** den Typ der Anwendungen (erlaubte, blockierte, alle), deren Statusänderungen im Ereignisprotokoll registriert werden sollen.

Achtung! Unabhängig von der in der Liste **Ereignisse registrieren** gewählten Option werden in der Logdatei alle Ereignisse erfasst, die mit einer Änderung der Liste der registrierten Anwendungen in Zusammenhang stehen (Ereigniscodes 3, 4, 5, 6, 7, 8, 13, 14).

---

6 Geben Sie im Feld Gleiche Ereignisse als ein Eintrag im Zeitabschnitt von den Wert in Minuten an. Standardmäßig ist 60 voreingestellt. Dadurch werden alle Ereignisse vom gleichen Typ (das heißt Ereignisse mit den gleichen Eigenschaften ausgenommen Zeit), mit einem einzigen Eintrag vermerkt.

Hinweis. Damit für jedes Ereignis ein eigener Eintrag erstellt wird, geben Sie für das Intervall den Wert 0 Minuten an.

---

7 Zum Einstellen der Parameter für die Aktualisierung des Ereignisprotokolls in Gruppe **Logdatei anzeigen**:

- Wählen Sie **Aktualisieren beim Klick auf „Aktualisieren"-Button** für eine manuelle Aktualisierung der Logdatei.
- Wählen Sie **Logdatei aktualisieren alle** für eine automatische Aktualisierung der Logdatei und geben Sie das Aktualisierungsintervall (in Sekunden) an.

8 Klicken Sie auf **Übernehmen**.

Auf diese Weise werden die Größe der Logdatei und des Archivs, der Typ der erfassten Ereignisse und die Art der Logdatei-Aktualisierung eingestellt.

Filter der Ereignisdarstellung einstellen

Die Parameter der Ereignisse, die im Bereich **Logdatei** angezeigt werden, können in den Einstellungen der Filter der Ereignisdarstellung konfiguriert werden. Die Möglichkeit zur Ereignisfilterung erlaubt es, konkrete Ereignisse zu finden, zum Beispiel Ereignisse, die mit einer bestimmten Anwendung oder IP-Adresse in Zusammenhang stehen.

Zum Einstellen des Filters der Ereignisdarstellung:

1 Klappen Sie im Hauptfenster im linken Bereich den Eintrag **Logdatei** auf.

2 Wählen Sie **Filter der Ereignisdarstellung**.

3 Um den Zeitabschnitt zu bestimmen, für welchen die Ereignisse angezeigt werden, wählen Sie in Gruppe **Anzeige eingrenzen** eine der angebotenen Optionen und geben Sie einen Zeitabstand an.

Abbildung 20. Fenster zum Einstellen des Filters der Ereignisdarstellung

4 Zum Einstellen weiterer Ereignisparameter (wie entfernte IP-Adresse und Port, lokaler Port, Protokoll, Dateiname des Programms und darzustellende Ereignistypen) setzen Sie in Gruppe **Ereignisparameter** die benötigten Werte ein.

5 Klicken Sie auf **Übernehmen**.

Zum Beispiel sollen Ereignisse angezeigt werden, die in Zusammenhang mit dem Torrent-Client uTorrent stehen und innerhalb des Zeitraums 1 April 2011 bis 15 April 2011 aufgetreten sind. Dazu:

1 Klappen Sie im Hauptfenster im linken Bereich den Eintrag **Logdatei** auf.

2 Wählen Sie **Filter der Ereignisdarstellung**.

3 Wählen Sie in Gruppe **Anzeige eingrenzen** in der Liste **Ereignisse anzeigen** den Eintrag **im Bereich** aus und geben Sie die benötigten Datumswerte an.

4 In Gruppe **Ereignisparameter**:

   - Wählen Sie in der Liste **Protokoll** den Eintrag TCP (Transmission control protocol) aus.
   - Geben Sie im Feld **Dateiname des Programms** den Wert `utorrent.exe` ein.
   - Stellen Sie sicher, dass in der Liste **Ereignisse anzeigen** der Eintrag **Alle** ausgewählt ist.

Abbildung 21. Filter der Ereignisdarstellung für den Torrent-Client uTorrent konfigurieren

5 Klicken Sie auf **Übernehmen**.

Dadurch werden im Bereich **Logdatei** nur Ereignisse erfasst, die den eingestellten Parametern entsprechen.

A

Glossar

B

Benutzerrechte

Die Rechte, die dem Benutzer für Einstellungen in der ViPNet Software auf seinem Netzwerkknoten zugewiesen sind. Die Anmeldung mit dem Administrator-Passwort hebt jegliche Einschränkungen der Benutzer-Anmeldung auf.

I

Interaktive Sicherheitsrichtlinie

Eine der Sicherheitsrichtlinien, die im Programm ViPNet Programmkontrolle verwendet werden. Bei dieser Richtlinie kann der Benutzer die weiteren Aktionen bei Verarbeitung von Anwendungsanfragen über die Arbeit im Netzwerk selbständig festlegen. Zu den interaktiven Sicherheitsrichtlinien gehören:

- „Erlaubt nach Benutzeranfrage";
- „Benutzer fragen";
- „Verboten nach Benutzeranfrage".

N

Netzwerkknoten Administrator

Person, die für die Konfiguration des Netzwerkknotens verantwortlich ist.

Nicht-interaktiver Modus

Modus der Verarbeitung von Anwendungsanfragen über die Arbeit im Netzwerk im Programm ViPNet Programmkontrolle. In diesem Modus kann „Programmkontrolle“ automatisch festlegen, welche Aktionen im Zuge der Verarbeitung einer Anwendungsanfrage durchzuführen sind.

V

ViPNet Netzwerk Administrator

Person, die für die Verwaltung des ViPNet Netzwerkes verantwortlich ist. Sie hat Zugriff auf den ViPNet Network Manager oder ViPNet Network Control Center und (oder) auf das ViPNet Key Certification Authority.

ViPNet Netzwerkknoten

Computer mit installierter ViPNet Software.

B

Index

A

B

L

N

P